



Privacy, Cyber & Data Strategy ADVISORY ■

DECEMBER 9, 2022

AI Regulation in the U.S.: What's Coming, and What Companies Need to Do in 2023

by [Dan Felz](#), [Kim Peretti](#), and [Alysa Austin](#)

Artificial intelligence (AI) technology is advancing exponentially and expected to dramatically change how companies operate on a global scale. Competitive pressures and advantages from AI optimization are driving business processes, and at times parts of entire industries, to increasingly rely on AI. Companies are dedicating more resources to developing, procuring, or acquiring AI tools and strategies to meet this need.

This has not escaped the attention of legislators and policymakers. This past year saw initial AI regulation models emerge, and 2023 promises to usher in a new wave of AI obligations for organizations. But despite the steady growth of global AI adoption, there is no comprehensive federal legislation on AI in the United States. Instead, the U.S. has a patchwork of various current and proposed AI regulatory frameworks. It is critical for organizations looking to harness this novel technology to understand these frameworks and to prepare to operate in compliance with them.

Industries Impacted by Increasing AI Dependencies

Even though it is generally felt that AI is becoming more prevalent in business, companies still at times see AI as something “other industries” are doing. As a result, many companies may not yet be aware of the extent of AI use in their operations. Companies should expect they are already using AI and start to consider how to manage AI regulatory risk.

Due to the sheer breadth of AI growth in recent years, examples of industries with considerable AI dependencies in daily operations include:

- **Financial Services, FinTech, and Payments:** Consumers can sign up for credit cards, apply for loans, open brokerage accounts, and seek financial or investing advice – all without interacting directly with a live human. Credit decisions may be made by AI algorithms, while advising can be done by robo-advisors. Payments are now protected by AI-powered fraud detection and security. FinTech develops new AI technology that, via acquisitions, finds its way throughout the financial services ecosystem.

This advisory is published by Alston & Bird LLP to provide a summary of significant developments to our clients and friends. It is intended to be informational and does not constitute legal advice regarding any specific situation. This material may also be considered attorney advertising under court rules of certain jurisdictions.

- **Insurance:** Insurance depends on underwriting and modeling, making it ripe for a variety of AI-use cases. Similar to financial services, insurance companies can use AI in underwriting decisions. AI also enables insurers to intake data over time to provide insurance on a more dynamic basis – like mobile apps that let consumers share real-time driving data for AI-powered technology to calculate premiums or safe-driving bonuses.
- **Automotive:** As AI continues to advance, it is expected to play an even greater role in the automotive industry, enabling vehicles to become even smarter and more capable. “Driver Assist” technology can make AI-powered decisions that alert inattentive drivers or take emergency action (like braking at intersections). Autonomous and self-driving vehicles will be powered by AI that operates vehicles in place of human drivers. AI is also increasingly used to improve vehicle safety, performance, and efficiency.
- **Logistics:** Similar to the automotive industry, logistics may see continued movement to autonomous delivery vehicles powered by self-driving AI. These may be on-road delivery vehicles, drones, or other forms of autonomous transportation technology. Additionally, AI is used to improve supply chain efficiency and optimize critical aspects of logistics, such as route planning and cargo loading.
- **Health Care & Medical Devices:** AI has the potential to revolutionize how health care is provided to patients. AI can improve patient care, reduce burdens on providers, and help avoid medical errors. AI can improve routine clinical tasks, such as assisting diagnoses, optimizing lab result or medical imaging analysis, and coordinating care management. On the device side, AI can monitor health data to automate interventions. Similarly, AI paired with wearables can track health markers like heart rate, activity, and sleep to personalize care and measure its effectiveness over time.
- **Retail, E-commerce, and Hospitality:** AI enables retailers and hospitality companies to provide a much more personalized relationship with customers. AI can create personalized online or in-store experiences, while also personalizing offers and promotions and potentially pricing. AI can also help optimize product recommendations – imagine, for example, showing your face to an in-store kiosk and receiving makeup and beauty product recommendations.
- **Marketing & Advertising:** Digital advertising already relies to a large extent on AI in campaign planning, bidding on paid media, and campaign measurement. As advertising moves away from cookies and individual-level tracking, AI-powered probabilistic modeling may become more important for companies to plan campaigns and measure effectiveness. AI also offers possibilities to dynamically personalize advertising messages in real time, potentially making ad campaigns more relevant and effective.
- **Manufacturing:** Manufacturing has largely moved to automated, robot-driven assembly processes. AI has the potential to automate additional parts of the manufacturing processes that had continued to rely on human input despite the robotics revolution, like quality control or safety inspections.
- **Media & Entertainment:** Many people may have experienced the moment where “the algorithm” of their content providers (like Netflix or Spotify) started to get their preferences right. AI enables personalized recommendations for viewing or listening. But AI is also enabling content creation itself. For example, electronic gaming already enables “worlds” where some characters’ behavior is partially created in real time by AI. This revolution may extend to further types of content and immersive experiences.

- **Education:** AI is being utilized in a variety of applications within the education industry, such as in personalized learning and in systems that assist teachers in creating and delivering lessons. The COVID-19 pandemic required remote-learning solutions that drove rapid growth in the EdTech sector. EdTech continues to be a field where new AI applications are developed for use in increasingly digital classroom settings.

U.S. AI Regulation to Expect in 2023

The rapid growth of AI has led to increasing focus on how best to regulate it. This year saw initial regulations emerge, and 2023 promises to provide further – and more general – AI compliance obligations. Several use-case-specific AI rules emerged in 2022. But more general AI regulatory initiatives may arrive in 2023: state data privacy law, FTC rulemaking, and new NIST AI standards.

Initial AI regulations in 2022

In the U.S., 2022 saw an initial approach to AI regulation emerge, focused on specific AI-use cases. The AI-use case most prevalently regulated was AI in recruitment or employment. For example, New York joined a number of states, including Illinois and Maryland, in regulating automated employment decision tools (AEDTs) that leverage AI to make, or substantially assist, candidate screening or employment decisions. Under New York's law, AEDTs must undergo an annual "bias audit," and results of this audit need to be made publicly available.

Similarly, the Equal Opportunity Employment Commission (EEOC) launched an [initiative on "algorithmic fairness"](#) in employment. As an initial measure in this initiative, the EEOC and Department of Justice jointly issued guidance on the use of AI tools in employee hiring. The guidance focused on AI that can, even if unintentionally, violate laws by screening out employees with disabilities. The EEOC [provided a technical assistance document](#) to assist companies with Americans with Disabilities Act compliance when using AI tools in hiring while reminding companies that they remain responsible for hiring decisions made by the AI they use.

State privacy laws – general requirements for consumer-facing AI in 2023

Moving beyond 2022, 2023 is likely to see some of the first general obligations that apply across AI-use cases, contained in privacy legislation passed by certain states. California, Connecticut, Colorado, and Virginia recently passed general data privacy legislation that goes into effect at various times in 2023. These laws contain provisions governing "automated decision-making," which includes technology that facilitates AI-powered decisions.

These statutes are privacy statutes and apply when AI processes personal information when making decisions that impact consumers. The new U.S. AI rules are inspired by similar provisions in the European Union's General Data Protection Regulation (GDPR). The GDPR requires heightened compliance when companies use technology like AI to solely make automated decisions that produce "legal ... or similarly significant" impacts on a consumer. Among their more salient obligations are the following:

- **Consumer Rights for AI-Powered Decisions:** State privacy laws grant consumers opt-out rights when AI algorithms make high-impact decisions – in the statutory language, decisions with "legal or similarly significant effects" on the consumer. These are generally defined as AI-powered decisions that grant or deny financial or lending services, insurance, housing, health care services, employment, educational opportunities, or basic necessities (like water). When AI profiles consumers to make these sorts of decisions, state privacy laws now require companies to provide opt-out rights.

- **AI Transparency:** Proposed Colorado privacy regulations would require companies to include AI-specific transparency in their privacy policies. Privacy policies would need to list all high-impact “decisions” that are made by AI and subject to opt-out rights. For each decision, the privacy policy would need to detail, among other things: (1) the logic used in consumer profiling that powers the AI decision; (2) whether the AI has been evaluated for accuracy, fairness, or bias; and (3) why profiles of consumers are relevant to the AI-powered decision. Additionally, in California, forthcoming regulations will determine how companies must give consumers “meaningful information” about the logic involved in AI-powered decision-making processes.
- **AI Governance via Impact Assessments:** When data processing presents a “heightened risk of harm to consumers,” companies must internally conduct and document a “data privacy impact assessment” (DPIA). This impacts AI because state privacy statutes require DPIAs for processing activities that often involve AI components, such as targeted advertising or consumer profiling, which may use AI to infer interests, behaviors, or attributes. Proposed Colorado regulations would require DPIAs to amount to what could be called “AI impact assessments,” documenting (1) explanations of training data; (2) explanations of logic and statistical methods used to create the AI; (3) evaluations of accuracy and reliability of AI; and (4) evaluations for fairness and disparate impact.

Federal AI regulation may be coming from the FTC

At the federal level, AI-focused bills have been introduced in Congress but have not gained significant support or interest. AI regulation does, however, appear to be potentially emerging from the Federal Trade Commission (FTC). In recent years, the FTC issued [two publications](#) foreshadowing increased focus on AI regulation. The FTC stated it had developed AI expertise in enforcing a variety of statutes, such as the Fair Credit Reporting Act, Equal Credit Opportunity Act, and FTC Act. These publications began to set forth ground rules for AI development and use, including:

- Make sure AI is trained using data sets that are representative, and do not “miss[] information from particular populations.”
- Test AI before deployment – and periodically thereafter – to confirm it works as intended and does not create discriminatory or biased outcomes.
- Ensure AI outcomes are explainable, in case AI decisions need to be explained to consumers or regulators.
- Create accountability and governance mechanisms to document fair and responsible development, deployment, and use of AI.

Parallel to its rulemaking, the FTC continued to use its existing authority under various existing consumer protection laws to expand AI enforcement. The FTC enforces the Fair Credit Reporting Act, Equal Credit Opportunity Act, Children’s Online Privacy Protection Act, and Section 5 of the FTC Act. These enabled the FTC to bring a number of recent AI-related enforcement actions, including:

- **Weight Watchers:** The FTC [entered a unique settlement](#) that required Weight Watchers to delete an entire AI algorithm it developed for a weight-loss app. The FTC contended that Weight Watchers marketed the app to children under 13 without parental consent and that children’s data had been collected in violation of the Children’s Online Privacy Protection Act. The FTC required Weight Watchers to delete all algorithms that had been trained using data from the weight-loss app.
- **Everalbum:** The FTC also [required online photo-storage platform Everalbum](#) to delete a facial-recognition algorithm it trained using photos users had stored on its platform. The FTC alleged Everalbum told users they

could turn off facial recognition features, but even if users did so, Everalbum continued to use their photos to train facial-recognition AI. The FTC contended this was deceptive conduct that violated the FTC Act and required Everalbum to delete its facial training data and the AI algorithms it had developed.

More recently, on August 22, 2022, the FTC issued [an advance notice of proposed rulemaking](#) (ANPR) aimed at addressing “commercial surveillance” and data security – but which also contained a full section exploring rulemaking for “automated decision-making systems.” The FTC specifically invited public comment on “whether it should implement new trade regulation rules” governing AI-powered technologies that make decisions impacting consumers. Among the issues the FTC seeks to clarify to aid in potential rulemaking are:

- Whether rules should require companies to take “specific steps to prevent algorithmic errors,” and what kind of error rates are generally prevalent in AI.
- Whether companies should have to certify that AI they use meets accuracy, validity, and reliability standards. If so, who should set the standards – the FTC, industry, or companies’ own published policies?
- Whether rulemaking should prohibit or limit companies from developing or using AI whose outcomes are “unfair or deceptive” under Section 5 of the FTC Act, and if so, whether the prohibition should be economy-wide or only apply in certain sectors.
- What kind of transparency companies provide to consumers about AI they use.

The ANPR marks an intentional shift toward a more holistic federal regulatory framework that addresses AI at all its phases: development, deployment, and use. While it is currently difficult to predict what the FTC’s AI rulemaking may look like, the FTC seems determined to proceed with the rulemaking process. Commissioners have stated they intend to move forward with rulemaking unless and until Congress passes comprehensive privacy legislation; barring such legislation, FTC rulemaking seems likely to move forward.

NIST proposes federal standards for trustworthy AI

In addition to the FTC, the National Institute for Standards and Technology (NIST) has begun work to standardize AI risks and an approach to managing them in a “trustworthy” manner. On July 29, 2021, NIST released an initial draft of an [AI Risk Management Framework](#) (AI RMF). By August 18, 2022, it had already been revised twice. The AI RMF is intended to provide guidance “to address risks in the design, development, use, and evaluation of AI products, services, and systems.” Although the AI RMF is nonbinding, like many NIST standards, it could potentially develop into an industry-standard approach.

The AI RMF is divided into two primary parts. The first part is a catalogue of characteristics that, if implemented in AI, would enable AI to be considered trustworthy because it minimizes key risks. These characteristics include:

- **Valid & Reliable:** AI is accurate, able to perform as required over time, and robust under changing conditions.
- **Safe:** AI does not cause physical or psychological harm, or endanger human life, health, or property.
- **Fair & Nonbiased:** Bias in results is managed at the systemic, computational, and human levels.
- **Explainable & Interpretable:** The AI’s operations can be represented in simplified format to others, and outputs from AI can be meaningfully interpreted in their intended context.

- **Transparent & Accountable:** Appropriate information about AI is available to individuals, and actors responsible for AI risks and outcomes can be held accountable.

The AI RMF's second part is an action framework designed to help companies identify concrete steps to manage AI risk and make AI trustworthy. It is built around a "Map – Measure – Manage" structure, where each concept covers a different phase in the AI planning, development, and deployment cycle.

- **"Map"** refers to the planning stage for AI – e.g., mapping the intended purpose of AI and its likely context of use – to identify likely risks and build AI to address risk while achieving intended functionality.
- **"Measure"** occurs during the development stage, when AI is built. It comprises identifying methods for building AI and metrics for measuring its performance – including metrics for evaluating AI's trustworthy characteristics.
- **"Manage"** refers to risk management after AI has been deployed. It includes monitoring whether AI is performing as expected, documenting risks identified through AI use, and developing responses to identified risks.

NIST's framework provides a unique combination of standards and a practical action framework a company can use to implement those standards into its own AI. NIST plans to submit the final version of the AI RMF to Congress in early 2023. In the meantime, NIST released an initial draft AI RMF Playbook, providing recommended actions on how organizations can implement the AI RMF.

What Companies Can Do to Get Ready for AI Regulation in 2023

While the regulatory approaches vary at the state, federal, and international levels, there are common themes found throughout all approaches that can guide compliance efforts. Companies that develop, deploy, or use AI systems may wish to consider the following steps to prepare for the new requirements coming online in the months ahead.

- **Know Your AI:** How many key operational decisions in your organization are made by, or materially depend on, non-human technology? Or to put it in terms an adverse party might one day use: Do you know which of your processes are run by robots? These are questions companies will increasingly be expected to answer by their management, boards, and regulators. Companies should begin mapping and assessing current and future AI dependencies. This can start from AI-use cases that many companies face irrespective of industry – such as AI tools used in candidate recruiting – and move out to industry-specific AI uses.
- **Lay the Groundwork for AI Adoption:** Companies should craft policies that govern how AI will be used in their organization. Policies should address dataset integrity, accuracy, transparency, foreseeable risks, and social impacts. These policies should allow for careful and regular monitoring to ensure AI systems do not lead to disparate and unfair outcomes.
- **Design Governance and Accountability Structures:** AI dependencies cut across corporate functions and will increasingly do so in the future as AI is integrated into more business processes. Companies should not presume that responsibility for AI will be organizationally obvious. Instead, companies may want to assume the opposite: if no one is in charge of AI policy, there may be no uniform organizational AI approach. Companies should consider designating a function – such as compliance – as responsible for setting and monitoring AI policy throughout the organization. This responsible function can then interface with business units to socialize AI policy throughout the organization so it becomes part of day-to-day operations.

- **Prepare to Communicate:** Companies that integrate automated decision-making into their business models should be prepared to respond to regulator and consumer inquiries sufficiently and accurately. Having a firm understanding of an AI system's mechanics is critical because companies may be expected to provide detailed explanations of the logic involved, in particular if individual personal information is used in the processing. A company that relies on third-party software should ask vendors and service providers for documentation for the underlying models that power the software's systems. Meticulous record keeping should be considered to demonstrate that a system does not lead to disparate outcomes.
- **Risk Assessments:** Companies deciding whether to implement a new AI system should consider a risk assessment (particularly if there could be a "heightened risk" to consumers) and cost-benefit analysis to determine whether the system is worth implementing, noting that bigger risks may justify a formal impact assessment. As risks are identified for particular use cases, companies should determine appropriate risk controls (technical, contractual, organizational) and start building controls into business units where risk can arise. Risk assessments may well become a standard and expected part of employing AI in organizations and will help companies do the legwork necessary to prepare to communicate about their AI.
- **Ongoing Governance:** There are a number of ways AI can enter a company. Companies may develop their own AI, they can license AI-powered technology from vendors, and they may acquire other organizations to obtain AI technology. Further, AI uses may change over time, and the impact that AI delivers may also increase. These considerations counsel for implementing ongoing, end-to-end governance structures for AI. Companies that have established information security programs, privacy compliance programs, risk management programs, Foreign Corrupt Practices Act programs, or similar compliance programs could consider applying these structures to AI governance.

You can subscribe to future *Privacy, Cyber & Data Strategy* advisories and other Alston & Bird publications by completing our [publications subscription form](#).

If you have any questions or would like additional information, please contact your Alston & Bird attorney or a member of our [Privacy, Cyber & Data Strategy Team](#):

Kimberly Kiefer Peretti
+1 202 239 3720
kimberly.peretti@alston.com

Daniel J. Felz
+1 404 881 7694
daniel.felz@alston.com

Katherine Doty Hanniford
+1 202 239 3725
kate.hanniford@alston.com

Amy Mushahwar
+1 202 239 3791
amy.mushahwar@alston.com

ALSTON & BIRD

Follow us: On Twitter  @AlstonPrivacy
On our blog – www.AlstonPrivacy.com

WWW.ALSTON.COM

© ALSTON & BIRD LLP 2022

ATLANTA: One Atlantic Center ■ 1201 West Peachtree Street ■ Atlanta, Georgia, USA, 30309-3424 ■ 404.881.7000 ■ Fax: 404.881.7777
BEIJING: Hanwei Plaza West Wing ■ Suite 21B2 ■ No. 7 Guanghua Road ■ Chaoyang District ■ Beijing, 100004 CN ■ +86.10.85927500
BRUSSELS: Rue Guimard 9 et Rue du Commerce 87 ■ 3rd Floor ■ 1000 Brussels ■ Brussels, 1000, BE ■ +32.2.550.3700 ■ Fax: +32.2.550.3719
CHARLOTTE: One South at The Plaza ■ 101 South Tryon Street ■ Suite 4000 ■ Charlotte, North Carolina, USA, 28280-4000 ■ 704.444.1000 ■ Fax: 704.444.1111
DALLAS: Chase Tower ■ 2200 Ross Avenue ■ Suite 2300 ■ Dallas, Texas, USA, 75201 ■ 214.922.3400 ■ Fax: 214.922.3899
FORT WORTH: Bank of America Tower ■ 301 Commerce ■ Suite 3635 ■ Fort Worth, Texas, USA, 76102 ■ 214.922.3400 ■ Fax: 214.922.3899
LONDON: 4th Floor ■ Octagon Point, St. Paul's ■ 5 Cheapside ■ London, EC2V 6AA, UK ■ +44.0.20.3823.2225
LOS ANGELES: 333 South Hope Street ■ 16th Floor ■ Los Angeles, California, USA, 90071-3004 ■ 213.576.1000 ■ Fax: 213.576.1100
NEW YORK: 90 Park Avenue ■ 15th Floor ■ New York, New York, USA, 10016-1387 ■ 212.210.9400 ■ Fax: 212.210.9444
RALEIGH: 555 Fayetteville Street ■ Suite 600 ■ Raleigh, North Carolina, USA, 27601-3034 ■ 919.862.2200 ■ Fax: 919.862.2260
SAN FRANCISCO: 560 Mission Street ■ Suite 2100 ■ San Francisco, California, USA, 94105-0912 ■ 415.243.1000 ■ Fax: 415.243.1001
SILICON VALLEY: 1950 University Avenue ■ Suite 430 ■ East Palo Alto, California, USA 94303 ■ 650.838.2000 ■ Fax: 650.838.2001
WASHINGTON, DC: The Atlantic Building ■ 950 F Street, NW ■ Washington, DC, USA, 20004-1404 ■ 202.239.3300 ■ Fax: 202.239.3333